UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,109	09/22/2003	Ram Anati	36437	7640

67801 7590 01/06/2009
MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
01/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/668,109	ANATI ET AL.	
	Examiner	Art Unit	
	MONJOUR RAHIM	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and argument field on ***18 September 2008.***
2. ***Claims 1-36*** are rejected under 35 U.S.C. 102/103(a) as being unpatentable over Atkinson et al. (US Patent No. 5511122), hereinafter Atkinson and in view of Douglas S. Daudelin (US PAT No. 4716376), hereinafter Daudelin.
3. U.S.C 101 claim rejection has been withdrawn.
4. Specification Objection has been withdrawn.
5. Claim Objection has been withdrawn.

Responses to the Argument

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. New reference has been used for the rejection.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 18, 17-30 are rejected under 35 U.S.C 102(b) as being anticipated by Atkinsonson (US Patent No. 5511122), hereinafter Atkinsonson.

As per **claim 1**, Atkinson discloses:

- **receiving an authentication datagram by said intermediate device** (Atkinsonson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the

established path of the first packet fragment or datagram fragment"), where "datagram" is dynamically sending, so inherently other side is receiving it, as claimed;

- protecting said datagrarn by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram (Atkinsonson, col 10, lines 26-33, "In order to permit any intermediate network gateway or router to authenticate the contents of the network frame, the public key for each host is published and the private key is kept private by that host. The sending host.sub.A 60 uses its public encryption key plus the data to generate a cryptographic signature which is embedded in the packet, see block 96. In this method, the public key of host.sub.B 83 is not requested or utilized in any manner");

- forwarding said datagram to said authentication server for authentication (Atkinsonson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment"), where datagram sent to the authentication system, as claimed.

As per **claim 2**, claim 1 is incorporated and further Atkinson discloses:

- wherein said intermediate device comprises a vendor world wide web site (Atkinsons, col 9, lines 26-30, "An intermediate router is any device which routes packets between any two communication devices. A gateway is an intermediate router which connects two subnetworks. Therefore, the terms may be used interchangeably throughout the detailed description").

As per **claim 3**, claim 2 is incorporated and Atkinson further discloses:

- wherein protecting comprises adding a signature associated with said vendor to said datagram (Atkinsons, col 9, lines 31-36, " Eventually, packets P.sub.1, P.sub.2 and P.sub.3 will migrate through subnetwork.sub.1 82 along the dashed lines in FIG. 2. In an architecture not shown, in which host.sub.B 83 is located within

subnetwork.sub.1 82, then host.sub.B 83 will receive the packets or fragments and reassemble them to gain access to the data and signature contained therein").

As per **claim 4,** claim 2 is incorporated and Atkinson further discloses:

- wherein protecting comprises encrypting said datagram(Atkinsons, col 9, lines 1-8, "Turning back to the steps in the host to host authentication method illustrated in FIG. 3, after performing the asymmetric encryption, host.sub.A 60 begins to transmit data, address and the digital signature to subnetwork.sub.1 82 via a gateway 62, see box 16'. The link/subnetwork communication protocol being used between host.sub.A 60 and subnetwork.sub.1 82 may vary with the particular type of host and network and thus, the location of the signature may vary").

As per **claim 5,** claim 1 is incorporated and Atkinson further discloses:

- wherein said intermediate device comprises a user computing device (Atkinsons, col 9, lines 26-30, "An intermediate router is any device which routes packets between any two communication devices. A gateway is an intermediate router which connects two subnetworks. Therefore, the terms may be used interchangeably throughout the detailed description"), where communication device is computing device.

As per **claim 6,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device adds a time stamp to said datagram (Atkinsons, col 11, lines 17-24, "This permits policy-based routing and usage-based accounting to be dependably implemented as illustrated in dashed box 112. Finally, the intermediate router transmits the reassembled packet to the next router or gateway, possibly refragmenting the packet if necessary, see dashed box 114").where timestamp is inherent.

As per **claim 7,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device adds a time stamp to said datagram (Atkinsons, col 11, lines 17-24, "This permits policy-based routing and usage-based

accounting to be dependably implemented as illustrated in dashed box 112. Finally, the intermediate router transmits the reassembled packet to the next router or gateway, possibly refragmenting the packet if necessary, see dashed box 114").where timestamp is inherent.

As per **claim 8,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device encrypts said datagram (Atkinsons, col 8, lines 7-13, ". A second method is to encrypt the output of a symmetric cryptographic hash function using an asymmetric encryption algorithm. A third method is to use a keyed asymmetric cryptographic hash algorithm. The above three methods have been utilized in the past to provide end-to-end application-layer authentication but have not been used to provide intermediate network authentication.").

As per **claim 17**, claim 1 is incorporated and Atkinson further discloses:

- wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication (Atkinsonson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment")

As per **claim 18**, Atkinson discloses:

- sending an encrypted datagram by secure computer communication from a vendor software to said remote authenticator; (Atkinson, col 6, lines 2-9, "When providing confidentiality using an asymmetric system, each party has two keys, one public and one private, and data is usually encrypted using the sender's private key and the recipients public key. When providing authentication using an asymmetric system, the data and the keys are used to generate a digital signature. That signature is verified by the recipient using the data received and the appropriate decryption keys");

- receiving said encrypted datagram by a remote authenticator (Atkinson, col 6, lines 1-9, "In a symmetric key system, the same key is used for encryption and decryption. When providing confidentiality using an asymmetric system, each party has two keys, one public and one private, and data is usually encrypted using the sender's private key and the recipients public key. When providing authentication using an asymmetric system, the data and the keys are used to generate a digital signature. That signature is verified by the recipient using the data received and the appropriate decryption keys");

- comparing said datagram or a hash thereof to a hash table at said server (Atkinson, col 2, lines 59-61, "transmitting the signature along with data to a first subnetwork in at least one packet, having a first packet size which is different from that of the transmitting host and thereby fragmenting the original packet into at least two packet fragments"), where differentiating is comparing, as claimed.

- generating a binary validation answer by said server without an associated explanation (Atkinson, col 7, lines 23-26, "All responses would use IP authentication. The Key Information Protocol would also use the host's public authentication key in the KIP response to enable the recipient to authenticate the response").

- **outputting validation answer** (Atkinsonson, col 7, lines 16-27, "To provide user asymmetric keys for encryption or authentication, it is suggested that a new service, the Key Information Protocol or KIP, be provided. This service would accept requests for user public keys and would respond only if such information were available. The "no key exists for that user" and "that user not valid here" cases would both cause an "invalid request" to be sent back to the requestor").

Claim 19 is rejected under the same reason set forth of claim 18 and Atkinson further discloses:

- datagram includes a secret code and wherein said secret code exists only on said authentication device (Atkinson, col 8, lines 62-67, "there is a potential for decreased size in the trusted code required to implement the authentication services. It

is usually easier to verify the correctness and trustworthiness of smaller amounts of code than larger amounts of code").

As per **claim 20**, claim 19 is incorporated and further Atkinson discloses;

- wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated (Atkinson, col 8, lines 58-68, "Each of these algorithms employ a secret or private key to perform a cryptographic process upon the items listed above and produce an authenticator code or digital signature. The key 54 used to perform this authentication is held secret so as to prevent others from counterfeiting this code or signature").

As per **claim 21**, Atkinson discloses:

- providing a code generating software (Atkinson, col 11 , lines 63-65 "Host.sub.B 83 will utilize a corresponding asymmetric algorithm to decode or verify the signature and thereby verify the authenticity of host.sub.A, see block 124.");

- providing at least one seed code for said software (Atkinson, col 8, lines 62-67, "there is a potential for decreased size in the trusted code required to implement the authentication services. It is usually easier to verify the correctness and trustworthiness of smaller amounts of code than larger amounts of code");

- destroying said seed immediately after generating said code set (Atkinson, col 7, lines 7-15, Hosts receiving an unauthenticated response should take note of the lack of authentication and may ignore unauthenticated responses if required by the security policy applicable to the subnetwork of the receiving host or take appropriate action. Hosts receiving a response containing incorrect authentication data should discard the response without processing it further. ");

-**forwarding said code set to said authentication device** (Atkinsonson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of

the first packet fragment or datagram fragment"), where datagram sent to the authentication system, as claimed.

- storing said code set or an indication thereof on an authentication device (Atkinson, col 8, lines 63-68, "Moreover, there is a potential for decreased size in the trusted code required to implement the authentication services. It is usually easier to verify the correctness and trustworthiness of smaller amounts of code than larger amounts of code"), where storing code is inherent.

Claims **22 and 23** are rejected under the same reason set forth in connection of claim 18 and 21.

As per **claim 24**, Atkinson discloses:

-generating one time code for the user for the session (Atkinson, col 2, lines 54-57, "utilizing the public key from the receiving host in combination with a private key from the sending host to generate a cryptographic signature; transmitting the signature along with data through a first subnetwork in at least one packet

- receiving an authentication datagram from said user (Atkinsonson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment"), where "datagram" is dynamically sending, so inherently other side is receiving it, as claimed;

- passing on said datagram for verification by a remote authentication server if at least an indication of said one time code that matches said user is provided with said datagram (Atkinson, col 3, lines 10-16, "reassembling the fragmented packets at an intermediate gateway or router; performing a verification of the cryptographic signature on the reassembled packet; retransmitting the fragmented packets through the first subnetwork; receiving at least one packet at the receiving host; and utilizing a public key for the sending host to verify the cryptographic signature.

Claim 25 is rejected under the same reason set forth in connection of claim 3.

As per **claim 26,** Atkinson discloses:

- matching said datagram or a hash of said datagram to a table (Atkinson, col 2, lines 59-61, "transmitting the signature along with data to a first subnetwork in at least one packet, having a first packet size which is different from that of the transmitting host and thereby fragmenting the original packet into at least two packet fragments"), where differentiating is comparing, as claimed.

- calculating a counter value from a matching position in said table (Atkinson, col 7, lines 3-7 "The HAK record's value is the authentication key certificate used for that host that the HAK record is associated with. No HAK records may exist that are not associated with a specific host");

- validating said authentication datagram based on an increase in said counter over a previous counter being within a certain limit (Atkinson, col 3, lines 42-46, "FIG. 4 is a flow chart illustrating a second preferred communications transaction between host.sub.A and host.sub.B in which both intermediate and end to end authentication may be conducted in a network which may employ fragmentation of datagrams.

Claims 27-29 are rejected based on inheritance:

As per **claim 27**, where authentication mechanism based encryption/decryption and it inherently checked or compare for number of try for successful or unsuccessful attempts to identify unwanted visitor.

As per **claims 28-29**, where check for the threshold settings is inherent.

Claim 30 is rejected under the same reason set forth of claim 26 and further "check for the threshold" is inherent.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-16, 31-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson (US Patent No. 5511122),), hereinafter Atkinson and further in view of Douglas S. Daudelin (US PAT No. 4716376), hereinafter Daudelin

As per **claims 9-16**:

Official notice is hereby taken it is well-known practice of encryption coding, such as using "temporary code", matching user with session ID, using of ActiveX, embedded software, caching data, secure connection between client and server, use of different path for different types of data.

The skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment.

As per **claim 31,** Atkinson does not teach "detecting a transmission of an acoustic multitone FSK signal"**.** However, Daudelin discloses:

- Detecting a transmission of an acoustic multitone FSK signal (Daudelin, col 3, lines 9-10, "FSK demodulator can optimally detect an FSK signal");

- receiving an acoustic signal (Daudelin, col 12, lines, "The constraints stem from the requirement that the received signal pass through the threshold value as the receiver's input frequencies are changed");

- converting the signal into a Hilbert-transform representation of the signal (Daudelin, col 4, lines, "The output of sampling circuit 160 is also applied on line 2 to a fixed phase shifting circuit 170 which includes a Hilbert transformer 4"), where "transformer 4" is the signal converter, as claimed;

- correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal (Daudelin, col 3, lines 48-56, "The demodulator includes a front end band pass filter 101 designed to remove out of band frequency components from an input signal applied on line 100 and

supply the filtered signal to a differential detector designated generally at 150 via a sampling circuit 160. The output of demodulator 150 is a d.c. signal plus a double frequency component which is applied to a low pass filter 102 and then to a threshold decision circuit 103"), where "filtered signal" is the converted signal correlating with the "input signal" where "input signal is the original FSK signal, as claimed;

- integrating said correlation over an interval (Daudelin, col 2, lines 29-32, "The 90 degree phase shift at the center frequency is achieved by a constant phase shift circuit which combines the output of a .+-.90 degree phase shifting circuit (advantageously a Hilbert filter) with the output of a scaling circuit having a variable gain factor K"), where, "combining the output" is the integrating and (Daudelin, col 11 , lines 27-32, "The number of counted samples depends upon the expected time interval (period) of each bit of the data signal which modulated the FSK carrier"),over an interval, as claimed;

- determining if a signal is present, based on a shareholding of a result of said integrating (Daudelin, col 13 , lines 45-50, "The difference generated by circuit 504 on line 506 is denominated a "threshold adjusted" signal and is applied to a decision circuit 501 which merely determines whether the threshold adjusted signal is positive or negative. The output from circuit 501 on line 500 represents the original FSK encoded data").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Atkinson with Daudelin's disclosure of transmitting signal from an "authentication card".

The modification would be obvious because one of the ordinary skills in the art would want to have a hacker-proof authentication by using mechanism of transmission of data using frequency shift key.

As per **claim 32**, claim 31 is incorporated and Atkinson does teach "detecting signal". However, Daudelin discloses:

- comprising further determining if a detected signal has a frequency within a certain frequency range (Daudelin, col 3, lines 9-13, "FSK demodulator can

optimally detect an FSK signal composed of any two frequencies which lie within a broad range of the two frequencies the demodulator is initially tuned to detect").

As per **claim 33**, claim 31 is incorporated and Atkinson does not teaches "detecting signal". However, Daudelin discloses:

- determining if a detected signal has a signal to noise ratio within a certain signal to noise ratio range (Daudelin, col 1, lines 31-42, " FSK input signal is formed which is phase shifted an amount that is a function of the instantaneous signal frequency, and the product of the original and phase shifted versions is then computed. The product contains a dc component equal to the cosine of the phase difference between the two signals, and a double frequency component. Ideally, the phase difference is chosen to be 90 degrees at the carrier frequency, in order to permit maximum noise immunity").
The same motivation applies as in claim 31, in this claim 33.

As per **claim 34**, claim 31 is incorporated and further discloses by Daudelin:

- comprising resampling said signal after said determining (Daudelin, col 3, lines 60-62, "The input to detector 150 consists of samples of the filtered FSK signal which are obtained by sampling the output of filter 101").
The same motivation applies as in claim 31, in this claim 34.

As per **claim 35**, claim 31 is incorporated and further discloses by Daudelin:

- wherein said threshold is noise dependent of the received signal (Daudelin, col 4, lines, " This arrangement gives the highest degree of noise immunity and also allows the ensuing threshold decision circuit 103 to operate by simply deciding if the value of the signal output from low pass filter 102 is greater or less than zero").
The same motivation applies as in claim 31, in this claim 35.

As per **claim 36**, claim 31 is incorporated and further discloses by Daudelin:

- calculating said interval based on a hardware characteristic of a producer of said acoustic signal (Daudelin, col 13, lines 66-67, and col 14, lines 1-11, "By virtue of the arrangement of FIG. 5, ... sum of (1) the current threshold and (2) a weighted average of the threshold adjusted signal at a pre selected time after successive (i.e., positive to negative and negative to positive) zero crossings. A typical value for .sigma. would be 1/100 of the maximum value reached by the threshold adjusted signal"), where interval was calculated by the circuit, as claimed.

The same motivation applies as in claim 31, in this claim 36.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (See form "PTO-892 Notice of reference cited).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MONJOUR RAHIM whose telephone number is (571)270-3890. The examiner can normally be reached on 5:30 AM - 3:30 PM (Mo - Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz, Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2434
Date: 12/08/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434